(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
2 octobre 2003 (02.10.2003)

PCT

(10) Numéro de publication internationale
WO 03/081546 A1

(51) Classification internationale des brevets[7] : G07F 7/10, G06F 1/00

(21) Numéro de la demande internationale :
PCT/FR03/00858

(22) Date de dépôt international : 18 mars 2003 (18.03.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
02/03743 26 mars 2002 (26.03.2002) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **OBERTHUR CARD SYSTEM SA** [FR/FR]; 102, Boulevard Malesherbes, F-75017 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **FINKELSTEIN, Vincent** [FR/FR]; 1, allée Gustave Courbet, F-95100 Argenteuil (FR). **ELISABETH, Fabrice** [FR/FR]; 27, rue de la Paix, F-92000 Nanterre (FR).

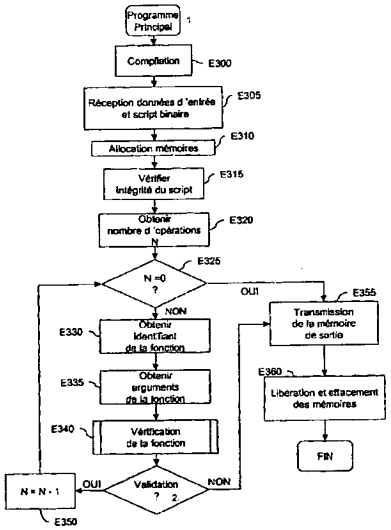
(74) Mandataire : **SANTARELLI**; 14, avenue de la Grande Armée, B.P. 237, F-75822 Paris Cedex 17 (FR).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE,

[Suite sur la page suivante]

(54) Title: METHOD AND DEVICE FOR AUTOMATIC VALIDATION OF A COMPUTER PROGRAM USING CRYPTOGRAPHY FUNCTIONS

(54) Titre : PROCEDE ET DISPOSITIF DE VALIDATION AUTOMATIQUE D'UN PROGRAMME INFORMATIQUE UTILISANT DES FONCTIONS DE CRYPTOGRAPHIE



1...MAIN PROGRAM
E300...COMPILATION
E305...BINARY SCRIPT AND INPUT DATA RECEPTION
E310...ALLOCATION OF MEMORIES
E315...VERIFY INTEGRITY OF SCRIPT
E320...OBTAIN NUMBER OF APPLICATIONS N
OUI...YES
NON...NO
E330...OBTAIN FUNCTION IDENTIFIER
E335...OBTAIN FUNCTION ARGUMENTS
E340...VERIFICATION OF FUNCTION
2...VALIDATION
E350...TRANSMISSION OF OUTPUT MEMORY
E360...RELEASE AND DELETION OF MEMORIES
FIN...END

(57) Abstract: The invention relates to a method for automatic validation of a computer program which can access a secure memory and a non-secure memory, said program using at least one coding function and at least one de-coding function. The inventive method comprises a verification step (E340) during which verification occurs to ensure that the each function which is adapted in order to read data from the secure memory and to produce data in the non-secure memory is a coding function and that all data produced by the coding function is stored in the secure memory.

(57) Abrégé : Ce procédé de validation automatique d'un programme informatique susceptible d'accéder à une mémoire sécurisée et à une mémoire non sécurisée, le programme utilisant au moins une fonction de chiffrement et au moins une fonction de déchiffrement, comporte une étape de vérification (E340) au cours de laquelle on vérifie . Que toute fonction adaptée à lire des données à partir de la mémoire sécurisée et à produire des données dans la mémoire non sécurisée est une fonction de chiffrement et que toute donnée produire par la fonction de déchiffrement est mémorisée dans la mémoire sécurisée.

WO 03/081546 A1